GLOBAL ALLIANCE AGAINST CHILD SEXUAL ABUSE ONLINE

United States

Policy target No. 1: Enhancing efforts to identify victims and ensuring that they receive the necessary assistance, support and protection

Operational Goal:	Increase the number of identified victims in the International Child Sexual Exploitation images database (ICSE database) managed by INTERPOL by at least 10% yearly
Operational Goal:	Establish the necessary framework for the criminalization of child sexual abuse online and the effective prosecution of offenders, with the objective of enhancing efforts to investigate and prosecute offenders
Actions ALREADY UNDERTAKEN	
Description of the actions <u>already undertaken</u>	**Identification of Victims** The National Center for Missing and Exploited Children (NCMEC) works closely with law enforcement officers in combating child exploitation. Law enforcement officers submit images and movies of children seized in child pornography cases to NCMEC's Child Victim Identification Program (CVIP) for review. This program has a dual mission: (1) to help prosecutors get convictions by proving that a real child is depicted in child pornography images; and (2) to assist law enforcement in locating unidentified child victims. The materials submitted are then screened through the Child Recognition and Identification System (CRIS), a specialized computer software program designed to efficiently determine which seized content appears to contain identified children. While reviewing contraband, CVIP analysts closely examine the images and videos submitted by law enforcement and document any clues that may lead to the location of an unidentified child victim. Once a location has been determined, the appropriate law enforcement agency may begin an investigation to rescue the child. Many children have been rescued from ongoing exploitation as a result of the cooperative efforts between CVIP and law enforcement. On a case-by-case basis, NCMEC also has been providing hash values for child pornography images of both identified and unidentified victims to the International Criminal Police Organization (INTERPOL) for inclusion in the International Child Sexual Exploitation images database (ICSE database). The Child Exploitation Investigations Unit of the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Cyber Crimes Center (C3), operates the Victim Identification Program (VIP), which was launched in December 2011. The VIP combines old-fashioned investigative techniques with cutting edge technology for the purposes of rescuing child victims of sexual exploitation. The victim identification process starts with the discovery of new child abuse material that depicts the sexual abuse of an unidentified minor or minors. HSI analyzes and enhances the material in order to identify clues that may lead to the identity of the victim, suspect, or geographic location. When enough clues come together to form a viable lead, a lead is sent out to the appropriate HSI field office for follow-up investigation. To date, the VIP has identified and rescued 79 child victims. DHS's Child Exploitation Investigations Unit also participates in the INTERPOL Specialist Group for Victim Identification (IPSG), which consists of over 40 countries working in collaboration to identify victims depicted in child pornography. In partnership with NCMEC, the Child Exploitation Investigations Unit has uploaded hundreds of identified series of child pornography to ICSE. The Child Exploitation Investigations Unit also has provided training regarding ICSE to law enforcement in other countries.

In 2008, the Federal Bureau of Investigation (FBI) launched "Operation Rescue Me," a child exploitation program focused on utilizing image analysis to determine the identity of child victims depicted in child sexual exploitation material. While most FBI investigations generally focus on obtaining leads and other information necessary to identify/prosecute subjects and offenders, the image analysis methods employed through Operation Rescue Me involve a concentrated effort to identify and subsequently "rescue" abused children. Since the program's inception, Operation Rescue Me has been responsible for the identification of 31 child victims depicted in numerous child pornography series being traded on the Internet. Candidate images for Operation Rescue Me arise from new child pornography series discovered by FBI field investigations, from forensic exams, or from nominations by NCMEC.

In 2004, the FBI began its Endangered Child Alert Program (ECAP), a new proactive approach to identifying unknown individuals involved in the sexual abuse of children and the production of child pornography. A collaborative effort between the FBI and NCMEC, ECAP seeks national and international exposure of unknown adults (referred to as John/Jane Does) whose faces and/or distinguishing characteristics are visible in child pornography images. These faces and/or distinguishing marks (i.e., scars, moles, tattoos, etc.) are displayed on the "Seeking Information" section of the FBI website as well as various other media outlets in the hope that someone from the public can identify them. As a result of ECAP, the faces of many Jane/John Does have been broadcast on U.S. television shows such as America's Most Wanted, America Fights Back, The Oprah Winfrey Show, and the O'Reilly Factor. Since the inception of ECAP, 24 John/Jane Does have been investigated, 15 of which have been successfully identified and subsequently prosecuted. These investigations have led to the identification of more than 29 child victims.

The United States Postal Inspection Service (USPIS) targets child exploitation offenders who utilize U.S. mail and the Internet to victimize children. Recently, USPIS has prioritized its enforcement efforts to target offenders who have direct contact with children through large scale operations. To date, in fiscal year 2013, USPIS has completed enforcement actions on over 110 subjects who were prior sex offenders, teachers, youth sport league volunteers, firefighters, police officers, and doctors. As part of its child exploitation enforcement efforts, USPIS works cooperatively with NCMEC to identify offenders and child victims. Since USPIS began to proactively concentrate on identifying child victims in seized child pornography material, it has identified 131 previously unidentified victims appearing in child exploitation material. In one case, USPIS arrested a middle school counselor in the State of Idaho who was sexually molesting children, producing images of that abuse, and distributing those images to offenders all over the world. Using image analysis and forensic evidence obtained from his computer, USPIS identified 50 child pornography production victims.

Services to Victims

Federal law requires a multidisciplinary child abuse team to be used when it is feasible to do so. The members of the team provide services in their professional roles, including medical diagnoses and evaluation services, telephone consultation services, medical evaluations related to abuse or neglect, psychological and psychiatric diagnoses and evaluation services, expert medical, psychological, and related professional testimony; case service coordination and assistance, training services for judges, litigators, court officers and others that are involved in child victim and child witness cases, in handling child victims and child witnesses. Nationwide, there are over 600 Child Advocacy Centers engaged in these efforts, supported by various combinations of federal, state and local funds.

U.S. federal law provides for mandatory restitution to victims in child pornography cases. Offenders are required to pay for the full amount of their victims' losses, including any costs incurred for (a) medical services relating to physical, psychiatric, or psychological care; (b) physical and occupational therapy or rehabilitation; (c) necessary transportation, temporary housing, and child care expenses; (d) lost income; (e) attorneys' fees, as well as other costs incurred; and (f) any other losses suffered by the victim as a proximate result of the child pornography offense.

Criminalization of Online Child Sexual Abuse Offenses

On both the federal and state level, the United States has a broad array of laws that criminalize online child sexual abuse offenses, including accessing with intent to view, possession, receipt, distribution, transportation, sale, advertising, and production of child pornography, and the online coercion and enticement of children to engage in prostitution or other sexual activity. Significantly, there is no statute of limitations for any federal child sex offenses, including all child pornography offenses. On the federal level, many of these offenses are subject to mandatory minimum sentences of imprisonment for first time offenders, including five (5) years imprisonment for the receipt, distribution, transportation, or sale of child pornography, ten (10) years imprisonment for coercion and enticement, and fifteen (15) years imprisonment for the advertising or production of child pornography.

Upon release from imprisonment, individuals convicted of online child sexual abuse offenses are subject to a mandatory minimum of five (5) years supervision by the court, and such supervision can extend for the remainder of their lives. The conditions of this supervised release often include restrictions on offenders' use of the Internet and/or the installation of software on their computers that monitors their computer usage. Additionally, for a minimum of fifteen (15) years, released offenders are required under federal law to publicly register as sex offenders in any U.S. jurisdictions in which they live, work, or go to school.

Investigatory Tools

U.S. law enforcement has a number of effective legal process tools that allow for the provision of subscriber and customer information, information regarding communications, the content of communications, and the real-time interception of such communications. U.S. law enforcement is required to abide by strict agency guidelines and laws in obtaining such evidence in order to ensure that these methods are used appropriately and judiciously. Additionally, with the appropriate authorizations, U.S. law enforcement is permitted to engage in proactive undercover operations both online and in person.

Cooperation Between Investigators and Prosecutors

In 2006, the U.S. Department of Justice instituted the Project Safe Childhood (PSC) initiative. PSC aims to combat the proliferation of technology-facilitated sexual exploitation crimes against children. The establishment of PSC reflected the view that the threat of sexual predators soliciting children for physical sexual contact is well-known and serious, and the danger of perpetrators who produce, distribute and possess child pornography is equally dramatic and disturbing. In 2011, PSC was expanded to incorporate all federal offenses involving the sexual exploitation of children. PSC is implemented through a partnership of federal, state, and local law enforcement agencies, and advocacy organizations, such as NCMEC. Under PSC, the number of federal child exploitation prosecutions has increased significantly, along with the number of federal, state, and local investigations and convictions, and more victims are being identified.

In 2008, the U.S. Department of Justice appointed a National Coordinator who serves as the Department's liaison with all federal agencies regarding the development and implementation of a national strategy to combat child sexual exploitation, and who works to ensure proper coordination among agencies involved in child exploitation prevention and interdiction. In 2010, the National Strategy for Child Exploitation Prevention and Interdiction was completed and establishes long-range goals for preventing child exploitation, including annual objectives for measuring the government's progress in meeting those goals. The goals for the Department of Justice are as follows: continue to partner closely with state, local, tribal, and nongovernmental entities, as well as other federal agencies and the private sector to implement the National Strategy in a coordinated fashion; build on the success of the PSC initiative; increase its commitment to a leadership role in finding a global solution to the transnational problem of the sexual exploitation of children; work toward improving the quality, effectiveness, and timeliness of computer forensic investigations and analysis; increase its commitment to effective and sophisticated training for prosecutors and investigators; continue to partner with Industry to develop objectives to reduce the exchange of child pornography; and explore opportunities to increase the education and awareness of federal, state, local, and tribal judges of the difficult issues involved in child sexual exploitation.

The Federal Inter-Agency Task Force on Missing and Exploited Children was created in 1995 and is comprised of representatives from numerous federal agencies, including the Department of Justice, Department of Defense, Department of Education, Department of Homeland Security, Department of Health and Human Services, Department of State, Department of the Interior, and the U.S. Postal Service. The Task Force convenes quarterly to coordinate efforts to combat all forms of child exploitation and discuss programs and policy that affect efforts to protect children.

NCMEC's Law Enforcement Committee is comprised of representatives from the private sector and the U.S. Department of Justice, FBI, DHS, U.S. Postal Inspection Service, U.S. Marshals Service, U.S. Secret Service, and military criminal investigative organizations, such as the Naval Criminal Investigative Service (NCIS). The Committee meets regularly to discuss investigative efforts in child exploitation cases.

Specialized Police Units and Prosecutors

The United States maintains specialized units of law enforcement personnel and prosecutors who are dedicated to the effective investigation and prosecution of online child sexual abuse offenses. On the federal level, these specialized units include: the Child Exploitation and Obscenity Section (CEOS) of the U.S. Department of Justice's Criminal Division, which prosecutes federal cases involving child sexual exploitation in conjunction with U.S. Attorney's Offices nationwide; the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit, which investigates Internet-facilitated and other crimes against children; and DHS-ICE-HSI's Child Exploitation Investigations Unit, which investigates Internet-facilitated and other crimes against children.

The U.S. Department of Justice also funds and provides training to Internet Crimes Against Children (ICAC) Task Forces located in every state of the United States. The ICAC Task Force program is a network of coordinated regional task forces engaged in helping state and local law enforcement agencies develop an effective response to cyber-enticement and child pornography cases. ICAC was developed in response to the increasing number of children and teenagers using the Internet, the proliferation of child pornography, and heightened online activity by predators seeking unsupervised contact with potential underage victims. As part of the PSC initiative, federal prosecutors have partnered with ICAC task forces that exist within their districts to

develop district-specific strategic plans to coordinate the investigation and prosecution of child exploitation crimes. The program is a national network of 59 coordinated task forces, with at least one in every state of the United States, representing over 2,000 federal, state, and local law enforcement and prosecutorial agencies. These agencies are engaged in proactive investigations, forensic investigations, and criminal prosecutions.

Cooperation Between Law Enforcement and Private Sector Actors

U.S. law enforcement agencies have relationships with private organizations focused on protecting children from exploitation, many of which they support with grant funding. The most notable example of such a public-private partnership is NCMEC, a private, non-profit entity that was created in 1994. Supported by significant funding from the U.S. Department of Justice, NCMEC assists victims of child exploitation, their families, and the professionals who serve them in a number of ways, including by serving as a clearinghouse of information about exploited children; operating an online and telephone Cyber Tipline that the public may use to report Internet- related child sexual exploitation; providing technical assistance to individuals and law-enforcement agencies in the prevention, investigation, prosecution, and treatment of cases involving exploited children; and offering training programs to law- enforcement and social-service professionals. To prevent duplication of efforts, NCMEC provides monthly deconfliction reports to United States Attorneys and ICAC task forces describing all law enforcement efforts stemming from Cyber Tipline reports in their states.

U.S. government agencies work closely with internet service providers (ISPs) and others from the private sector to explore ways to improve efforts to combat child sexual exploitation, and to ensure that legal process requests in child exploitation investigations are handled effectively and efficiently. In October 2011, the U.S. Department of Justice convened a panel of experts from Facebook, Microsoft, and NCMEC to explore ways to prevent and deter child sexual exploitation. The national summit, titled "A Call to Action: Protecting Children from Sexual Exploitation," brought together attendees from law enforcement, industry, and child advocacy organizations.

"Project Vic" is a proof-of-concept project that is intended to promote the investigation of child pornography images that depict unidentified victims, and improve the quality of law enforcement- exchanged data, standardize law enforcement data formats, and promote data exchange efforts in child pornography investigations. The project's participants consist of federal and state law enforcement agencies, the International Centre for Missing & Exploited Children (ICMEC), NetClean, Microsoft, Hubstream, Thorn, and the University of Illinois at Chicago. The project is relying on the use of robust, updated forensic and image categorization tools and new technologies in order to allow computer forensic analysts to review and analyze computer media containing large collections of child pornography in a more automated and efficient manner. As a result, child pornography images that depict victims who have not been identified can be more easily isolated for further investigation. To date, all participating law enforcement agencies have made an initial submission of images to a central repository, and attended training focused on categorization methods and the use of NetClean; over forty law enforcement officers/investigators have been trained on categorization and robust hashing techniques at a hands-on lab; the initial submissions of images have been analyzed to eliminate duplicates and redistributed to the agencies for categorization; and agencies are currently engaged in the process of reviewing and categorizing these images

Actions that WILL BE UNDERTAKEN	
Description of the actions that <u>will be undertaken</u> and timeframe	NCMEC has recently agreed to directly upload child pornography images to ICSE, including images of both identified and unidentified victims. NCMEC is currently finalizing the details of this agreement with INTERPOL - NCB Washington. Shortly thereafter, in 2013, it is anticipated that NCMEC will begin furnishing a significant amount of information to ICSE regarding identified series of child pornography. DHS-ICE-HSI intends to expand its successful VIP program in 2013 by training 24 additional agents at 12 HSI field offices in victim identification techniques and technologies. As part of Operation Vic, an additional fifty law enforcement officers/investigators will be trained on categorization and robust hashing techniques at a hands-on lab in April 2013. In 2013, law enforcement agencies will be submitting more images to the central repository. The U.S. Department of Justice is currently preparing an update to the 2010 National Strategy for Child Exploitation Prevention and Interdiction, which will be completed by June 2013. In developing this updated strategy, the Department will be engaging in discussions regarding next actions

Policy target No. 2: Enhancing efforts to investigate cases of child sexual abuse online and to identify and prosecute offenders

Operational Goal:	Improve the joint efforts of law enforcement authorities across Global Alliance countries to investigate and prosecute child sexual abuse online
Actions ALREADY UNDERTAKEN	
Description of the actions already undertaken	In recent years, the United States has spearheaded several investigations of private, online child pornography groups consisting of members from around the world. These investigations have required joint investigative efforts with several international law enforcement partners. A recent, successful example of such efforts is "Operation Delego," an investigation conducted by DHS-ICE-HSI that was launched in December 2009 and involved extensive international cooperation to identify and apprehend members of the private, online bulletin board Dreamboard. Dreamboard was created and operated to promote pedophilia and encourage the sexual abuse of very young children, in an environment designed to avoid law enforcement detection. Members traded graphic images and videos of adults molesting children 12 years-old and under, often violently, and collectively created a massive private library of images of child sexual abuse. The international group prized and encouraged the creation of new images and videos of child sexual abuse - numerous Dreamboard members sexually abused children, produced images and videos of the abuse, and shared the images and videos with other members of Dreamboard. Evidence obtained during the operation revealed that at least 38 children across the world were suffering sexual abuse at the hands of the members of the group. Dreamboard members employed a variety of measures designed to conceal their criminal activity from detection by law enforcement. Members communicated using aliases or "screen names," rather than their actual names. Links to child pornography posted on Dreamboard were required to be encrypted with a password that was shared only with other members. Members accessed the board via proxy servers, which routed Internet traffic through other computers so as to disguise a user's actual location and prevent law enforcement from tracing Internet activity. Dreamboard members also encouraged the use of encryption programs on their computers, which password-protect computer files to prevent law enforcement from accessing them in the event of a court-authorized search. Operation Delego involved extensive international cooperation to identify and apprehend Dreamboard members abroad. A total of 72 individuals have been charged as a result of Operation Delego. To date, 59 of the 72 charged defendants have been arrested in the United States and abroad. Through coordination between DHS-ICE-HSI, the U.S. Department of Justice, Eurojust, the European Union's Judicial Cooperation Unit, and dozens of law enforcement agencies throughout the world, 20 Dreamboard members across five continents and fourteen countries have been arrested to date outside the United States, including two of the five lead administrators of the board. Those countries include Canada, Denmark, Ecuador, France, Germany, Guatemala, Hungary, Kenya, the Netherlands, the Philippines, Qatar, Serbia, Sweden and Switzerland. Numerous foreign investigations related to Operation Delego remain ongoing. The location and arrest of Dreamboard members abroad have led to the capture and investigation of other global targets. Operation Delego is a spinoff investigation from leads developed through "Operation

Nest Egg," the prosecution of another online group dedicated to the sharing and dissemination of child pornography. Operation Nest Egg was a spinoff investigation developed from leads related to another international investigation, "Operation Joint Hammer," which targeted transnational rings of child pornography trafficking.

Training

The U.S. Department of Justice, Criminal Division's Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT), drawing on the expertise of experienced prosecutors from CEOS, the Civil Rights Division and its Human Trafficking Prosecution Unit, and the United States Attorney's Offices, has designed and executed technical assistance and training programs overseas to strengthen international capacity to combat trafficking in persons, including child sex trafficking and child exploitation offenses. OPDAT assisted Brazil in the drafting of a child pornography law, enacted in November 2008, which makes possession of child pornography a felony, the first time it has been so criminalized in Brazil. OPDAT provided technical assistance and training to Russia in addressing its serious child exploitation and pornography problems. As a result, the Russian MVD (Interior Ministry) agreed to participate in the FBI's Innocent Images Global Task Force; Russian child pornography investigations increased tenfold; and in July 2009, Russia enacted legislation with severe penalties for crimes against minors, including sexual abuse.

CEOS Attorneys and computer forensic specialists provide training on issues pertaining to online child sexual abuse offenses to prosecutors, law enforcement officers, and victim service providers from the federal, state, and local levels. Such training is provided at national and local conferences around the country, including the Annual Crimes Against Children Conference in Dallas, Texas, where prosecutors, law enforcement officers and victim service providers are trained together. Such joint training is common and reflects the close working relationships and partnerships relied upon in child exploitation investigations and prosecutions in the U.S. In addition, CEOS distributes newsletters on a quarterly basis to federal prosecutors that provide guidance concerning numerous issues pertaining to all federal child exploitation crimes. CEOS, in partnership with OPDAT and the State Department, also regularly provides training for foreign delegates on child exploitation offenses as part of the State Department's International Visitor Program.

These training sessions range from providing an overview of U.S. child exploitation laws, including child protection statutes, and how to investigate and prosecute human trafficking cases successfully. In addition, CEOS attorneys travel around the world to train foreign law enforcement, prosecutors, investigators, and service providers involved in the investigation and prosecution of sexual exploitation crimes against children, including extraterritorial sexual exploitation of children by Americans.

In January 2013, CEOS organized presentations by Microsoft, DHS- ICE-HSI, and NCMEC regarding the use of PhotoDNA technology to combat child pornography at an Expert Meeting sponsored by the Group of Eight (G8) Roma-Lyon Group High Tech Crime Sub-Group, which was attended by both domestic and foreign ISPs, and at a meeting of the Law Enforcement Projects Sub-Group (LEPSG). For more information on PhotoDNA, see additional information reported below for Policy Target No. 4.

The International Centre for Missing & Exploited Children (ICMEC), working with INTERPOL, has trained police in 121 countries in investigative techniques in computer-facilitated crimes against children.

Existing International Law Enforcement Efforts

The United States participates in the Virtual Global Taskforce (VGT), which is

	comprised of international law enforcement agencies and private sector partners from around the world working together to fight child abuse online. The VGT strives to make the Internet a safer place, identify, locate and help children at risk, and hold perpetrators accountable. The VGT was established in 2003 and includes the U.S. (DHS-ICE-HSI), United Kingdom (Child Exploitation and Online Protection Centre), Canada (Royal Canadian Mounted Police), Australia (Australian Federal Police), Italy (Postal and Communication Police), the Ministry of Interior for the United Arab Emirates, and INTERPOL as its current members. The VGT is intended to augment, not supplant, existing law enforcement initiatives and international relationships related to child exploitation issues. DHS-ICE-HSI is the exclusive U.S. representative to the VGT, and serves as the current chair of the VGT. The FBI's Innocent Images International Task Force (IIITF) became operational in 2004. The IIITF consists of online child sexual exploitation investigators from around the world and includes more than 100 task force officers from 44 different countries, including the United Kingdom, Norway, Finland, Ukraine, Belarus, Australia, Thailand, the Philippines, Croatia, Latvia, Germany, the Netherlands, New Zealand, Canada, Sweden, Fiji, Cyprus, Iceland, Denmark, and Panama. Each year the task force hosts a new member training session that brings newly invited task force officers to the United States to attend a six-week training session where they work side-by- side with special agents of the FBI at the Major Case Coordination Unit. Task force officers remain an integral part of the task force once they return to their home countries, and IIITF has allowed for the real-time transfer of information from and to the FBI, and between task force members and their countries. The IIITF also conducts an annual case coordination meeting where task force members come together in a central location to share best practices and coordinate transnational investigations between members. In coordination with NCMEC, DHS-ICE-HSI has established Virtual Private Network (VPN) connections for direct access to CyberTipline reports in Australia, Brazil, Canada, Denmark, Germany, Guatemala, Hong Kong, Japan, Mexico, The Netherlands, New Zealand, Philippines, Singapore, Thailand, and the United Kingdom. Discussions are ongoing to expand VPN connections to other countries interested in obtaining such access. In 2009, CEOS helped organize an international symposium through the G8 Roma-Lyon Group titled "Global Symposium for Examining the Relationship Between Online and Offline Offenses and Preventing the Sexual Exploitation of Children." The symposium was held at the University of North Carolina in Chapel Hill, North Carolina and brought together researchers and other experts from around the world who have worked with child pornography offenders and victims. The symposium was designed for these experts to share their research and individual findings, and develop consensus on the risks to children and society posed by child pornography offenders and also to identify gaps in research and knowledge. Among the most notable points of consensus developed include a finding that there is sufficient evidence of a relationship between possession of child pornography and the commission of contact offenses against children to make it a cause of acute concern, and that the greater availability of child sexual exploitation materials has stimulated the demand and production of even more extreme, sadistic, and violent images of children and infants. The findings and gaps in research were incorporated into a report written by CEOS, entitled "Report to LEPSG on the 'Global Symposium for Examining the Relationship Between Online and Offline Offenses and Preventing the Sexual Exploitation of Children.'" On May 30, 2009, the G8 Ministers of Justice and Home Affairs issued a declaration titled "The Risk to Children Posed by Child Pornography Offenders," which

	specifically recognizes the findings made by the experts at the symposium as noted in the report written by CEOS. **Public Awareness Campaigns** In 2008, the Online Safety and Technology Working Group (OSTWG) was established and its participants included representatives from the business community, public interest groups, and federal agencies. OSTWG's purpose was to evaluate industry efforts and develop recommendations to promote online safety for children through education, labeling, and parental control technology. OSTWG also evaluated and developed recommendations on industry efforts to prevent and respond to criminal activity involving children and the Internet. In June 2010, the OSTWG submitted a report to Congress and the Assistant Secretary for Communications and Information of its findings and made recommendations on how to increase online safety measures. A copy of OSTWG's report, "Youth Safety on a Living Internet," is available here: http://www.ntia.doc.gov/legacy/advisory/onlinesafety/index.html See additional information reported below for Policy Target No. 3
Actions that WILL BE UNDERTAKEN	
Description of the actions that will be undertaken and timeframe	CEOS and INTERPOL are currently working together to create and sustain a common global platform for international joint investigations that standardizes the methodologies and principles for case coordination, victim identification, and press - including country points of contact, evidence sharing, live video conferencing capabilities, enforcement action priority, and timing. CEOS is currently developing a protocol to streamline the process by which mutual legal assistance treaty (MLAT) requests received from foreign countries are reviewed and addressed in order to ensure that requests in child exploitation cases are handled more efficiently. Through the United States' participation in the G8 Roma-Lyon Group Law Enforcement Projects Sub-Group (LEPSG), the United States is partnering with the United Kingdom to coordinate a follow-up symposium to the 2009 Global Symposium for Examining the Relationship Between Online and Offline Offenses and Preventing the Sexual Exploitation of Children. In October 2013, the United Kingdom will host the Global Symposium "Preventing the Online Sexual Exploitation of Children" in London. The U.S. Department of Justice is currently preparing an update to the 2010 National Strategy for Child Exploitation Prevention and Interdiction, which will be completed by June 2013. In developing this updated strategy, the Department will be engaging in discussions regarding next actions.

Policy target No. 3: Enhancing efforts to increase public awareness of the risks posed by children's activities online, including grooming and self-production of images that results in the production of new child pornography that may be distributed online

Operational Goal	Share best practices among Global Alliance countries for effective strategies to inform the public about the risks posed by online, self- exploitative conduct in order to reduce the production of new child pornography
Actions ALREADY UNDERTAKEN	
Description of the actions already undertaken	Description of the actions already undertaken A number of federal agencies and non-governmental organizations (NGOs) in the United States conduct public awareness campaigns utilizing a variety of mediums to alert the public about the threat of and demand for the sexual exploitation of children. The campaigns are intended to raise public awareness about the crime and to act as a deterrent for potential violators. The FBI's Safe Online Surfing (S.O.S.) Program is a national Internet safety program designed to help students recognize potential dangers associated with the Internet, email, chat rooms and social networking sites. This initiative was launched nationally in the Fall of 2009. The program addresses and defines topics serious in nature, such as seduction, child pornography, solicitation, exploitation, obscenity and online predators. Students take web-based quizzes and review specific web sites aimed at promoting online safety. Approximately 60,000 students have participated throughout the United States in the program. More information regarding S.O.S. can be found at: https://sos.fbi.gov/ The FBI's Violent Crimes Against Children Program produced "A Parent's Guide to Internet Safety" to inform parents of the risks children face online of encountering adults who might sexually exploit them and how to recognize child behaviors that might indicate the child is at risk for being exploited. The guide is available in hard copy and online at: www.fbi.gov/publications/pguide/pguidee.htm. The FBI also posts a list of safety rules for children using the Internet at: www.fbi.gov/kids/k5th/safety2.htm. The Federal Trade Commission manages OnGuardOnline.gov, which is a federal government website designed to help individuals be safe, secure, and responsible online. The website contains a section dedicated to protecting children online and includes information and materials directed to children in order to help raise their awareness of the real world consequences to online activities. For an example, see the brochure "Heads Up: Stop Think Connect," at: http://www.onguardonline.gov/articles/pdf-0002.pdf. Additionally the U.S. Secretary of Education joined the Chairs of the Federal Trade Commission and the Federal Communications Commission in launching Net Cetera, a guide for parents to help them talk to their children about Internet safety. The guide is designed to help parents address three areas related to their children's online activities: inappropriate conduct, inappropriate contact, and inappropriate content. The aim is to protect children against, among other things, online predators and pornography. The guide, "Net Cetera: Chatting with Kids About Being Online," is available at: http://www.onguardonline.gov/sites/default/files/articles/pdf/pdf- 0001.pdf. Through its PSC initiative, the U.S. Department of Justice has developed public service announcements (PSAs) in both English and Spanish to help prevent online crimes against children. These PSAs were produced collaboratively by the Department's Office of Juvenile Justice and Delinquency Prevention, the Hispanic Communications Network, and the Internet child safety organizations INOBTR ("I Know Better") and

	iKeepSafe. One series of PSAs alerts parents about the risk of online sexual exploitation and encourages them to supervise their children's use of the Internet. The other targets potential online predators, warning them of the serious criminal penalties awaiting those who victimize children. These PSAs are available at: http://www.iustice.gov/psc/video.html NCMEC's NetSmartz Workshop program has interactive, educational safety resources for children ages 5 to 17. Through age-appropriate activities, games, videos and safety presentations, NetSmartz prepares children to behave responsibly when confronted with issues such as cyberbullying, inappropriate content, online exploitation, revealing too much information, sexting and scams. These free materials are available at: http://www.netsmartz.org The Office on Women's Health of the U.S. Department of Health and Human Services maintains the web site www.girlshealth.gov. This website for adolescent girls includes information regarding safe surfing and chatting or instant messaging on the Internet, and safety in online communities. OSTWG's report, "Youth Safety on a Living Internet," provides a comprehensive list of NGOs engaged in promoting Internet safety to children, and details industry-provided Internet safety programs from Facebook, YouTube, Yahoo!, and others. See Addenda A and B to the Subcommittee on Internet Safety Education section at: http://www.ntia.doc.gov/legacy/advisory/onlinesafety/index.html
Actions that WILL BE UNDERTAKEN	
Description of the actions that <u>will be undertaken</u> and timeframe	The U.S. Department of Justice is currently preparing an update to the 2010 National Strategy for Child Exploitation Prevention and Interdiction, which will be completed by June 2013. In developing this updated strategy, the Department will be engaging in discussions regarding next actions

Policy target No. 4: Reducing as much as possible the availability of child pornography online and reducing as much as possible the re-victimization of children whose sexual abuse is depicted

Operational Goal:	Encourage participation by the private sector in identifying and removing known child pornography material located in the relevant State, including increasing as much as possible the volume of system data examined for child pornography images.
Operational Goal:	Increase the speed of notice and takedown procedures as much as possible without jeopardizing criminal investigation
Actions ALREADY UNDERTAKEN	
Description of the actions already undertaken	NCMEC's CyberTipline receives leads and tips from the public and ISPs regarding suspected crimes of sexual exploitation committed against children. The CyperTipline is authorized by Congress and operated in partnership with the FBI, DHS-ICE-HSI, the U.S. Postal Inspection Service, the ICAC task forces, the U.S. Secret Service, CEOS, as well as other state and local law enforcement entities. More than 1.7 million reports of suspected child sexual exploitation have been made to the CyberTipline between 1998 and December 2012. Reports are continuously triaged to help ensure children in imminent danger get first priority. The CyberTipline reporting mechanism assists law enforcement and prosecutors in their detection, investigation and prosecution of child sexual exploitation crimes. The CyberTipline helps make law enforcement's efforts more efficient and maximizes the limited resources available in the fight against child sexual exploitation. The value of the CyberTipline as a source of leads for law enforcement has been greatly enhanced by collaboration with ISPs. In addition to referring CyberTipline reports to law enforcement for potential investigation, NCMEC engages with the Internet industry on voluntary initiatives to reduce child sexual exploitation online. ISPs are required by federal law to report information concerning child pornography on their systems to the NCMEC CyberTipline. ISPs can be fined up to $150,000 the first time they willfully fail to comply with the reporting requirement, and up to $300,000 for all subsequent willful failures to report. While ISPs are required to report instances of child pornography that come to their attention (for example, through a complaint received by a customer), they are not obligated to take proactive steps to look for child pornography on their systems. Nevertheless, many companies voluntarily search for such criminal activity on their servers. NCMEC offers resources to ISPs to assist with their voluntary efforts to reduce child pornography on their servers. Through NCMEC's Hash Value Sharing Initiative, subject to certain conditions, domestic and foreign ISPs can partner with NCMEC to receive a list of MD5 hash values that represent the "worst of the worst" images of apparent child pornography. Additionally, through NCMEC's URL Initiative, ISPs are provided access to a list of URLs for active website pages containing apparent child pornography, which is updated daily. Lastly, in 2009, Microsoft donated PhotoDNA technology to NCMEC to help disrupt the spread of known child sexual abuse images online. Microsoft's PhotoDNA technology works by creating a unique signature for a digital photograph, like a fingerprint, that calculates the essential characteristics of the image. That signature, also known as a "hash," can then be compared with the digital signatures of other images to efficiently and reliably find matching signatures. PhotoDNA was designed to

	be usable by online service providers and others to be able to identify matches across very large data sets. Unlike other common "hashing" technologies, PhotoDNA was designed to consistently match signatures even in cases where the image has been resized or similarly altered. Microsoft granted NCMEC the legal right to sublicense this technology for free to domestic and foreign ISPs interested in taking proactive steps to identify and eliminate child pornography from their servers. After an ISP has licensed PhotoDNA, NCMEC can also provide access to a set of NCMEC PhotoDNA signatures pursuant to a separate legal agreement. These NCMEC-generated PhotoDNA signatures are derived from apparent child pornography images that have been reported by U.S.-based ISPs to law enforcement via NCMEC's CyberTipline. In 2012, Microsoft made its PhotoDNA image matching technology available to law enforcement agencies at no cost to help enhance their child sex abuse investigations. PhotoDNA is now available through a version of NetClean Analyze, a free technology already used by law enforcement in child sex abuse investigations in many countries worldwide. This version includes functionality to support connections between NetClean Analyze and the Child Exploitation Tracking System (CETS), a collaborative global law enforcement program supported by Microsoft technology for child pornography investigations. PhotoDNA is also being integrated into CETS. CETS helps law enforcement agencies follow hundreds of suspects at a time and eliminate duplication, making it more efficient for the agencies to follow up on leads, collect evidence and build cases against suspected child pornographers. CETS is currently used by agencies in Australia, Brazil, Belgium, Canada, Italy, the United Kingdom and the United States. Additionally, certain law enforcement agencies with the technical capacity and resources required to manage PhotoDNA source code integration themselves can license the technology directly for use in child sexual exploitation investigations. At this time, the Netherlands Forensics Institute and the New Zealand Department of Internal Affairs have licensed the PhotoDNA source code. Since 2006, federal law has required that images of child pornography remain in the care, custody, and control of the government or the court during criminal proceedings, thereby minimizing further dissemination of the images. Accordingly, defense attorneys are required to review child pornography materials at government facilities in most cases and they are not permitted to retain copies of the material to aid in the preparation of their cases.
Actions that WILL BE UNDERTAKEN	
Description of the actions that <u>will be undertaken</u> and timeframe	In 2013, NCMEC will be expanding the number of child pornography images included in its MD5 and PhotoDNA signature hash sets, which are available to domestic and foreign ISPs for their use in taking voluntary steps to reduce the availability of online child pornography. The U.S. Department of Justice is currently preparing an update to the 2010 National Strategy for Child Exploitation Prevention and Interdiction, which will be completed by June 2013. In developing this updated strategy, the Department will be engaging in discussions regarding next actions.